RFID Kullanan Biyometrik Tabanlı Akıllı ATM

Gokul.S, Kukan.S, Meenakshi.K, Vishnu Priyan S S, Rolant Gini J, M.E.Harikumar
Elektronik ve Haberleşme Mühendisliği Bölümü Amrita
Mühendislik Okulu, Coimbatore
Amrita Vishwa Vidyapeetham, Hindistan
gokulsridharan1999@gmail.com, s.kukan77@gmail.com, meeru.krishh@gmail.com, vishnu32510@gmail.com,
j_rolantgini@cb.amrita.edu, me_harikumar@cb.amrita.edu

***Özet* - Günümüz dünyasında nakit para çekmek için ATM kullanımı artmıştır. Aynı zamanda, hırsızlık ve soygun vakaları da artmıştır, bu da güvenlik için ek özellikler sağlayan çok daha güvenli ATM'ye ihtiyaç duyulmasını gerektirmektedir. Bu çalışmada, erişim için RFID ve parmak izi yetkilendirmesine dayalı olarak çalışan güvenlik tabanlı akıllı ATM amaçlanmaktadır. RFID numarası ve parmak izi detayları kullanıcıdan alınır, ardından tanınan kart numarası, yetkilendirme durumu ve erişim konumu, veritabanı ayrıntılarıyla gerçekliğini kontrol etmek için aktarılır. Bilgi, alınan veritabanı ayrıntılarıyla doğrulandıktan sonra, ilgili hesap sahibi yetkilendirmenin geçerli olup olmadığı mesajını alır. Erişimin yeri, saati ve tarihi de hesap sahibine bildirilir. Buna ek olarak, yangın ve kırılma durumunda anında bildirimde bulunan titreşim ve alev sensörleri yerleştirerek güvenliği artırır. Tam güvenlik sağlamak için, ATM kartına erişen kişinin yüzü de - bir kamera kullanılarak - şüphe durumunda kullanılabilecek erişim saati ve tarihi ile makineye kaydedilir.**

Anahtar Kelimeler-IoT; RFID; esp8266; mikrodenetleyici; parmak izi sensörü; gömülü sistem; sinyal işleme.

I. GIRIŞ

Otomatik Vezne Makinesi (ATM), banka müşterilerine banka şubesine gitmelerine gerek kalmadan hesaplarına erişerek nakit para çekme ve diğer finansal ve finansal olmayan işlemleri gerçekleştirme olanağı sağlayan bilgisayarlı bir makinedir. ATM'ler ilk olarak 1967 yılında Londra'da kullanılmaya başlanmış ve 50 yıl sonra bu makineler ülke çapında kullanılmaya başlanmıştır. ATM gelişiminin büyümesi Tablo I'de özetlenmiştir [1].

ATM noktaları birçok yerde elverişli bir şekilde konumlandırılmıştır. Herhangi bir bankanın ATM'sine yılın 365 günü, 7x24 saat nakit çekmek için erişilebilir. Yurtdışına seyahat ediliyorsa, kart, kişinin seyahat ettiği ülkenin para birimini ATM'den çekmek için kullanılabilir. Bir ATM'nin kullanımı sadece PIN (Kişisel Kimlik Numarası) bilen kişi ile sınırlıdır. ATM'nin en büyük faydası şubeye gitmek için zaman kazandırması ve işlem yapmak için kuyrukta bekleyerek zaman kaybetmeye gerek bırakmamasıdır. ATM olanakları, çeşitli işlemler için anında bankacılık seçeneği sunar. Nakit çekme ve hesap bakiyesini kontrol etmenin yanı sıra, modern ATM'ler bir bankada sabit mevduat açmak, cep telefonu şarj etmek, gelir vergisi ödemek, nakit para yatırmak, sigorta primi ödemek, kişisel kredi başvurusunda bulunmak, nakit transferi yapmak, fatura ödemek, tren bileti rezervasyonu yapmak vb. için kullanılır,

TABLO I. ATM'NİN ZAMAN ÇİZELGESİ - BİR BİLGİLENDİRME

Dönem	Geliştirme
1988 - 1994 (Başlangıç dönemi)	Nakit yatırma ve nakit çekme
1995 - 1999 (İlk gelişmeler)	Quiry'de mini tablolar ve denge
2002 - 2004 (Genişletilmiş gelişmeler)	Çek defteri talebi, Fon transferleri ve Dokunmatik ekran olanakları
2004 - 2006 (Üçüncü taraf hizmetleri)	Demiryolu ve Havayolu bilet rezervasyonu. Fatura ödeme (elektrik, geniş bant gibi). Cep telefonu için şarj etme
2007'den itibaren	Özelleştirilmiş ATM hizmetleri

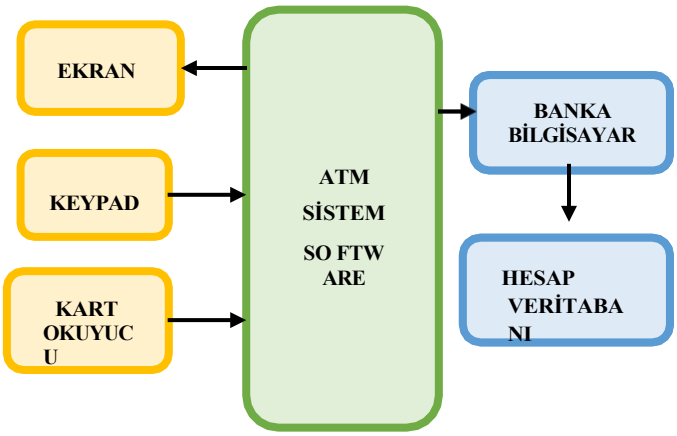
Hindistan genelinde çok sayıda ATM merkezi bulunduğundan ve ATM hırsızlığı vakalarının sayısı her geçen gün arttığından, her merkezin güvenliği sağlanmalıdır. Sonuç olarak, ATM'deki güvenlik görevlilerine ek olarak, daha güvenilir güvenlik yöntemleri gereklidir. Şok edici bir şekilde, sadece Ocak 2020 ile 16 Nisan 2020 arasında Hindistan'daki çeşitli ATM merkezlerinde yaklaşık 50 hırsızlık vakası rapor edilmiştir; bunlardan birkaçı ATM'nin sökülmesini de içermektedir [2]. Bu nedenle, bu proje temel olarak güvenli, kolay erişilebilir ve emniyetli bir ATM inşa etmeyi amaçlamaktadır.

II. MEVCUT ATM SISTEMI

Mevcut ATM sistemi iki tür hizmet sunmaktadır. İlki, müşteriye talep ettiği nakit parayı sağlar ve alınan miktar ve hesap bakiyesi hakkında bir rapor içeren bir mesaj gönderir. İkincisi ise daha gelişmiş olup kullanıcıdan para yatırma işlemini kabul etmekte, kredi kartı ile ödeme imkanı sağlamakta ve kullanıcıya işlem ve hesap bilgileri hakkında bir mesaj göndermektedir.

ATM'nin mevcut sistemi Şekil 1'de özetlenmiştir. ATM'ye giriş, kart okuyucu ve tuş takımı gibi giriş cihazları aracılığıyla tanınmaktadır. Kart okuyucu, kullanıcının kart numarasını tanımlayan karttan veri okumak için kullanılan bir giriş cihazıdır. Kart, ATM kartının arka tarafındaki manyetik şerit ile bağlantı kurulduktan sonra hesap bilgilerini yakalayan kart okuyucu üzerinde kaydırılır veya bastırılır. Bu bilgi, kart sahibiyle ilgili ayrıntıları almak için verileri kullanan ana sunucuya aktarılır. Kullanıcıdan bilgi almak için, şu anda işlemci ile arayüzlenen yaklaşık 48 tuş içeren bir tuş takımı bulunmaktadır. Kart, bir Kişisel Kimlik Numarası (PIN) kullanılarak tanınır. PIN yetkilendirildikten sonra, kullanıcı ATM tarafından sağlanan herhangi bir hizmeti

tuş takımı. Güvenliği sağlamak için, her kartın benzersiz bir PIN kodu vardır ve PIN kodu ana işlemciye şifrelenmiş biçimde gönderilir.



Şekil 1. Mevcut sistemin blok diyagramı.

A. Mevcut bir ATM sisteminin avantajları

- Sistem, işlem gerçekleşir gerçekleşmez kart sahibine bir mesaj gönderir.
- Sistem, kullanıcının ATM'ye gelmesine gerek kalmadan, kartın PIN kodunu bilen herkesin karta erişebileceği bir esneklik sağlamaktadır.
- Her kartın benzersiz bir PIN kodu vardır.
- PIN şifrelenmiş bir biçimde işlemciye gönderilir.

B. Mevcut bir ATM sisteminin dezavantajları

- Suçlular ATM'lere küçük kameralar yerleştirerek hesap bilgilerini ve kişisel kimlik numaralarını kaydedebilir ve bu da dolandırıcılık ve soygun risklerini artırır.
- Kullanıcı, bu işlem hakkında herhangi bir mesaj almaz. karta yetkisiz erişim.
- Kullanıcı, cihazın konumu hakkında bilgi alamaz. Hırsızlık durumunda karta erişim.
- ATM'ye erişen kişinin yüzü, daha fazla depolama alanına ihtiyaç duyan CCTV'de video olarak saklanır.
- ATM kartı üzerinde kart numarası, CVV gibi kartın kötüye kullanımını destekleyen bilgiler görüntülenir.

Bahsedilen çeşitli senaryolara ışık tutarak, mevcut ATM'lerde PIN yerine kimlik doğrulama için alternatif yöntemlerin kullanılması [3], [4], makinedeki titreşimin algılanması üzerine uyarı mesajları gönderilmesi [5], ATM'ye erişen kişileri kaydetmek için kameralara sahip olunması [6] gibi gelişmeler gerekmektedir. Bu makale temel olarak ATM'ye giriş olarak RFID etiketi ve parmak izi kullanmayı amaçlamaktadır. Kart sahibi, erişimin geçerli olup olmadığına bakılmaksızın kimlik doğrulama durumu, ATM'nin konumu, erişim tarihi ve saati ile ilgili bir mesaj aldığından, kart sahibinin kartının kötüye kullanılması hakkında bilgi edinmesine yardımcı olur. Buna ek olarak, titreşim ve alev sensörleri, ilgili departmanları uyararak hırsızlık ve yangın kazalarını önler.

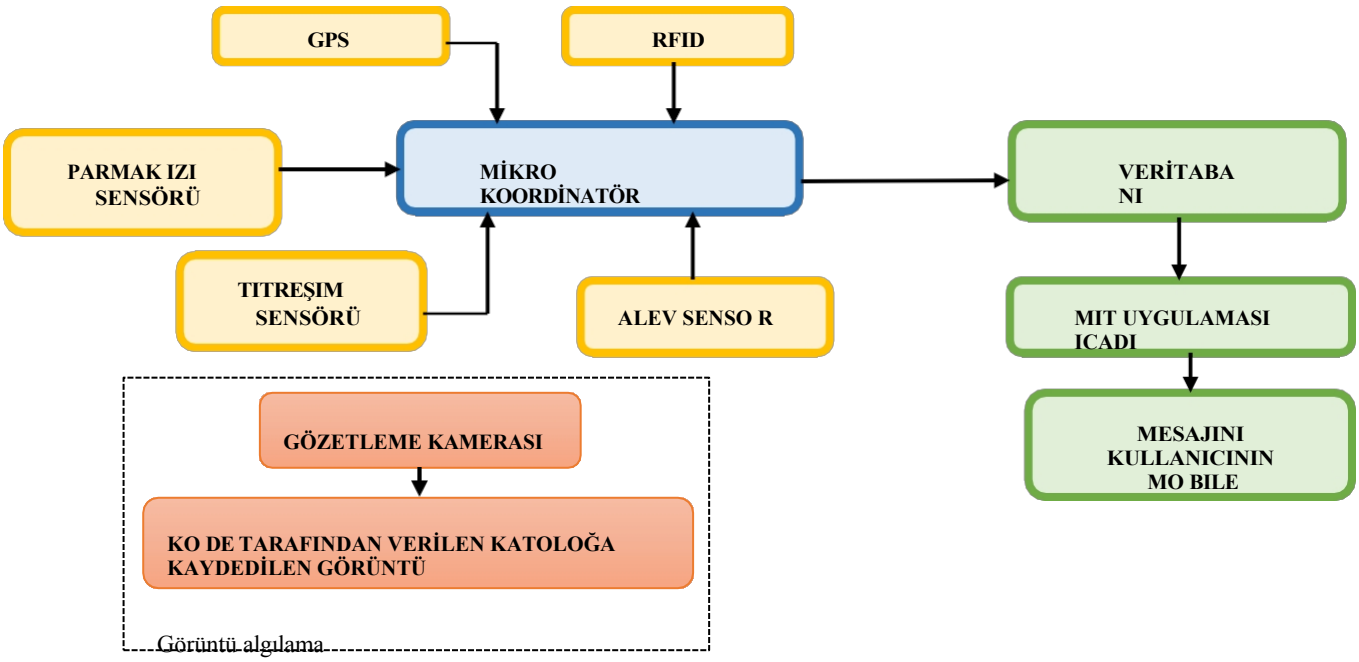
olaylar. Bu projede mesaj gönderme yöntemlerinin uygun maliyetli olduğuna dikkat etmek önemlidir. Ayrıca, ATM'deki kullanıcının yüzünü yakalamak için bir kamera kullanmak, CCTV kameralarının gerektirdiği gibi istenmeyen depolama alanını azaltmaya yardımcı olur.

III. ATMOSFER IÇIN ÖNERILEN SISTEM

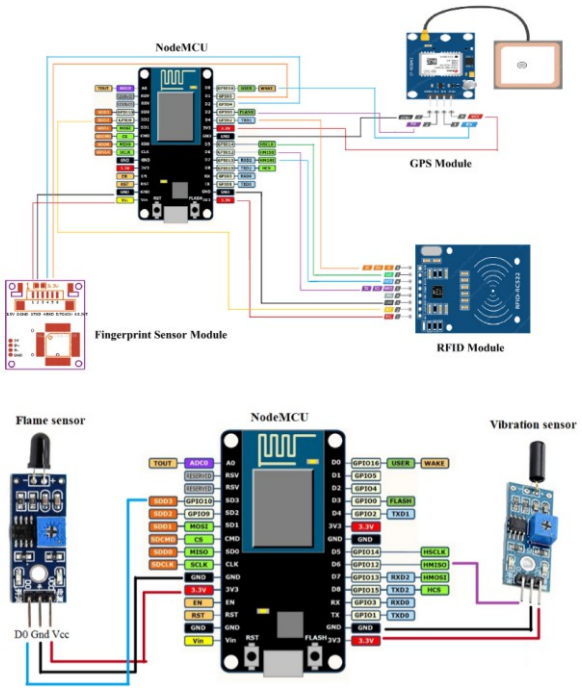
Önerilen sistem, normal kartların kullanıcının kart numarasını içeren RFID kartlarla değiştirildiği mikrodenetleyici tabanlı bir ATM'dir. PIN kullanmak yerine, yetkilendirme için kullanıcının parmak izi kullanılır. Bu nedenle, kişi ATM'nin yakınındaysa, kartı RFID tarayıcı tarafından taranır ve sistem ilgili kartın geçerli parmak izini bekler. ATM'nin parmak izi sensörü tarafından geçerli bir parmak izi algılanırsa, karta kayıtlı telefon numarasına "Erişim izni verildi" şeklinde bir mesaj gönderilir. Öte yandan, geçersiz bir parmak izi tanınırsa, ilgili kartın kullanıcısı "Erişim izni verilmedi! Birisi bu karta erişmeye çalıştı" şeklinde bir mesaj alır. Erişimin sağlanıp sağlanmadığına bakılmaksızın, kart sahibi erişimin saati, tarihi ve yeri hakkında da bilgi alır. İstenmeyen video akışının depolanmasını en aza indirmek için, ATM içindeki kişilerin görüntüleri, ATM'de hırsızlık durumunda ilgili bankaya ve kart sahibine yardımcı olan bir kamera aracılığıyla veri tabanına kaydedilir. ATM'de yangın çıkması durumunda, önerilen sistem otomatik olarak ATM'nin GPS koordinatları ile birlikte itfaiyeye bir mesaj gönderir. Ayrıca, birisi ATM'yi kırmaya çalışırsa, sistem otomatik olarak ATM'nin GPS konumu ile birlikte polis karakoluna bir mesaj gönderir [7]. Bu nedenle, önerilen sistem bankaya yardımcı olmak ve ATM'de güvenliği sağlamak için ATM'nin güvenliği alanında gerekli birçok yönü birleştirmektedir. Şekil 2'deki blok diyagramı önerilen sistemin çalışmasını göstermektedir.

Önerilen sistem RFID tarayıcı ve kartları, parmak izi sensörü [8], GPS modülü, NodeMCU, alev sensörü ve titreşim sensörü gibi donanım bileşenlerini kullanmaktadır. Sensörlerden alınan girdiyi işlemek için Arduino, sensör okumalarının değerlerindeki değişiklikleri izlemek için bir uygulama oluşturan MIT app inventor, mesaj göndermek ve bulut depolama için firebase gibi yazılım platformları kullanmıştır.

NodeMCU'nun kullanılmasının ana nedeni, içinde gerekli değerleri bulut veritabanına, bu durumda firebase'e göndermeye yardımcı olan yerleşik bir WiFi modülüne sahip olmasıdır. Kullanıcının kartı olarak kullanılan MFRC522 tabanlı RFID okuyucu modülü ve ilgili kart okuyucu, kısa bir mesafeden veri aktarmak için elektromanyetik alanlar kullanır.
13.56MHz. Parmak izini kullanıcıdan kimlik doğrulama için bir şifre olarak almak için bir R307 parmak izi modülü kullanılır. Parmak izi işleme temel olarak kayıt ve eşleştirme olmak üzere iki unsur içerir. Parmak izi kaydında, her kart sahibinin parmağını, sistemin işlemek için parmak görüntülerini kontrol ettiği ve parmağın bir desenini oluşturduğu sensöre iki kez yerleştirmesi gerekir. Kaydedilen parmak izi saklanır. Eşleştirmede, ATM erişimi sırasında kullanıcı parmağını optik sensöre yerleştirir, ardından sistem parmağın bir desenini üretir ve bunu parmak kütüphanesi şablonlarına kayıtlı parmaklarla karşılaştırır.



Şekil 2. Önerilen sistemin Önerilen sistemin blok diyagramı.



Şekil 3. Önerilen sistemin devre şeması Önerilen sistemin devre şeması

Buna ek olarak, işlemin gerçekleştiği yerin konumu, erişimin tarihi ve saati gibi ayrıntıları almak için bir GPS modülü kullanılır. ATM'nin enlem ve boylamını kullanıcıya göndermenin temel avantajı, ATM'nin konumunun tam olarak bilinmesi ve aynı konumda birçok ATM merkezi olması durumunda karışıklıkların önlenmesidir. Firebase, bu projede kullanılan bulut veritabanıdır.

Kart bilgileri, yetkilendirme durumu, ATM'nin konumu, erişim saati ve tarihi gibi hayati parametreler ATM'den güncellenir. Veritabanını kullanmanın temel amaçlarından biri, son işlemle ilgili ayrıntıları almak ve ilgili kart sahibine mesaj göndermektir. Bir web uygulaması geliştirme ortamı olan MIT App Inventor kullanılarak, kart sahibine ilgili ayrıntılarla mesaj göndermek için firebase'den değerlerin alındığı bir mobil uygulama oluşturulmuştur. Ayrıca, kazalara ve hırsızlıklara karşı önlem almak için ATM'de güvenliği sağlamak amacıyla alev ve titreşim sensörleri kullanılmıştır. Ayrıca, ATM'yi kullanan kullanıcıların yüzlerinin görüntülerini yakalayan görüntü işleme tekniklerini uygulamak için Python kullanılmıştır. Depolanan görüntüler gelecekte doğrulama için veritabanına gönderilir. Görüntünün tanınması ve veri tabanına aktarılmasıyla, ATM kartı hırsızlıklarında ve parmak izi dolandırıcılıklarında artış olduğu için ATM'nin güvenliği artırılmıştır.

IV. Sonuçlar ve Tartışmalar

Devre Şekil 3'te gösterildiği gibi ayarlandığında, kod mikrodenetleyiciye beslenir. İçlerinde kart numaraları bulunan RFID kartları olduğunu ve ilgili parmak izlerinin gelecekteki yetkilendirme için saklandığını varsayarsak, RFID kart numarası, kullanıcı kimliği, erişimin yeri, erişim durumu (yetkilendirmenin geçerli olup olmadığı) vb. gibi değerleri takip etmek için bir uygulama oluşturulmuştur. Bu uygulama "MIT app inventor" adlı bir araç tarafından oluşturulmuştur. Bu, kartın ATM'ye erişiminden sonra kullanıcıya mesaj göndermek için kullanılan araçtır.

Şekil 4. Mobil Uygulama Geliştirilen mobil uygulamanın simgesi/logosu.

Geliştirilen mobil uygulamanın başlangıç simgesi Şekil 4'te gösterilmiştir. Uygulamanın ana sayfası ve yönü Şekil 5'te gösterildiği gibi görülebilir. Bir işlem veya bir işlem girişimi yapıldığında, ilgili değerler, geliştirilen android uygulaması Şekil 4 aracılığıyla alınan firebase'de (kullanılan veritabanı) güncellenir. Bunu takiben, RFID kart numarası, kullanıcı kimliği, erişim konumu, erişim durumu, alev ve titreşim sensörü durumu için ilgili değerler, ilgili etiketlerin metnini değiştirerek uygulamada güncellenir. Her etiket bir ATM'yi temsil etmektedir.

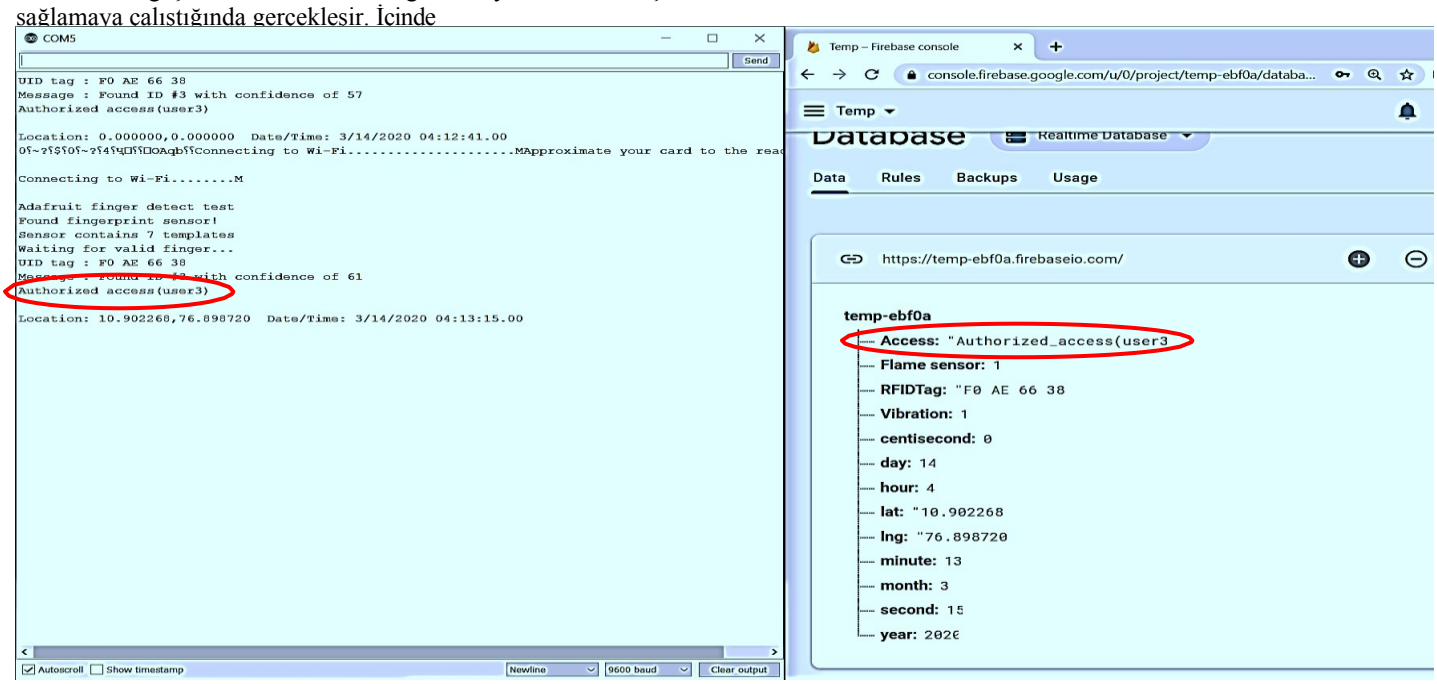
Şekil 5. Uygulamanın ana sayfası. Uygulamanın ana sayfası.

Gerçek zamanlı çalışma için geliştirilen sistemde Tablo II'de gösterildiği gibi dört olası durum meydana gelebilir. İlk durum, bir kullanıcı geçersiz bir kart kullandığında veya bu kartla erişim sağlamaya çalıştığında gerçekleşir. İçinde Bu durumda ATM kullanıcıyı geçersiz bir kullanıcı olarak görüntüler. İkinci durum, kullanıcı geçerli bir kart kullanarak sisteme eriştiğinde ve kart için ilgili geçerli parmak izini verdiğinde gerçekleşir. Bu durumda, erişim izni verilir ve RFID kart numarası, konum ve erişim zamanı değerleri Firebase'de güncellenir ve uygulama aracılığıyla alınır. İlgili kartın sahibinin kayıtlı telefon numarasına, karta erişilen ATM'nin GPS koordinatları ve Şekil 6 ve Şekil 7'de gösterildiği gibi diğer kimlik bilgileriyle birlikte "erişimin yetkilendirildiğini" belirten bir mesaj gönderilir.

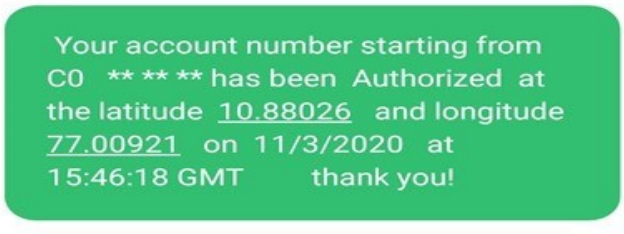
TABLO II. TEST DURUMLARI

Senaryolar	Vaka 1	Vaka 2	Vaka 3	Vaka 4
RFID Kart	Geçersiz	Geçerli	Geçerli	-
Parmak izi	-	Geçerli	Geçersiz	-
Mesaj	Gönderilmedi	Gönderildi	Gönderildi	Gönderildi

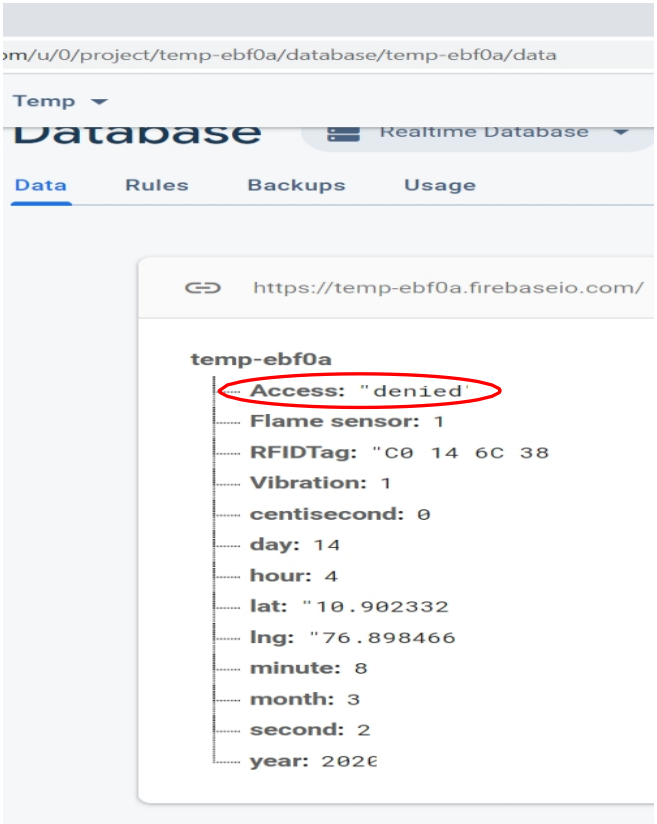
Üçüncü durum, sisteme erişim için geçerli bir kart verildiğinde ancak ilgili kart için geçersiz bir parmak izi verildiğinde gerçekleşir. Sistem daha önce kaydedilen kart için ilgili parmak izini beklediğinden bu durumda erişim verilmez. RFID kart numarası, konum ve erişim zamanı değerleri Firebase'de güncellenir ve uygulama aracılığıyla alınır. Firebase & IDE'deki yanıt, reddedilen durum için Şekil 8'de gösterilmiştir. Kart sahibinin kayıtlı telefon numarasına, kartın erişim için denendiği ATM'nin GPS koordinatları ve Şekil 9'daki gibi saat, tarih vb. diğer kimlik bilgileriyle birlikte "erişimin reddedildiğini" belirten bir mesaj gönderilir.



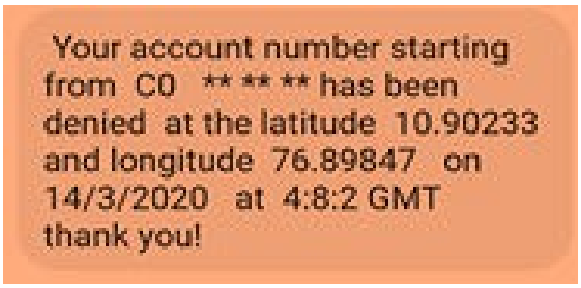
Şekil 6. Yetkilendirilmiş bir vaka için Firebase ve IDE ekranı. Yetkilendirme her iki platformda da kırmızı renkli dairelerle gösterilmiştir.



Şekil 7. Yetkili bir durumda kart sahibi tarafından alınan mesaj



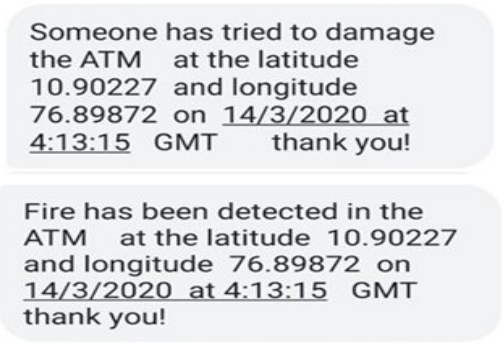
Şekil 8. Kırmızı daire ile gösterilen erişim reddi vakası için Firebase verileri.



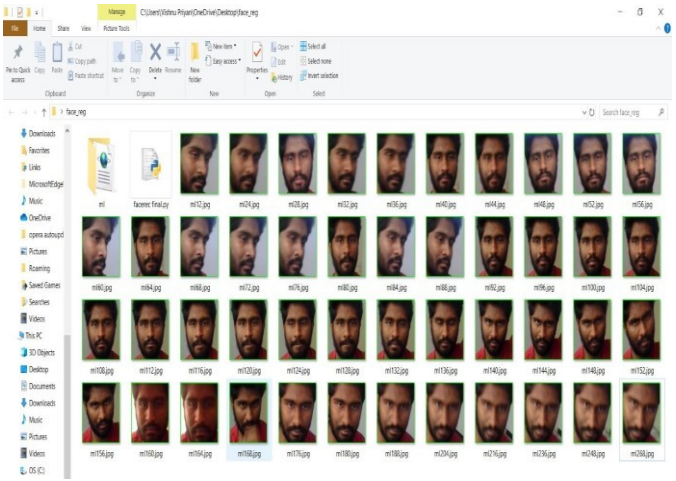
Şekil 9. Reddedilen bir durumda kart sahibi tarafından alınan metin mesajı.

Dördüncü durum, alev ve titreşim sensörleri yerleştirerek ATM'de güvenliği sağlamaktır. Birisi ATM'yi kırmaya veya zarar vermeye çalışırsa, Şekil 10'da gösterildiği gibi ATM'nin GPS konumu ile eylem hakkında polis karakoluna bir mesaj gönderilir. Yangın durumunda, itfaiye istasyonuna bir mesaj gönderilir.

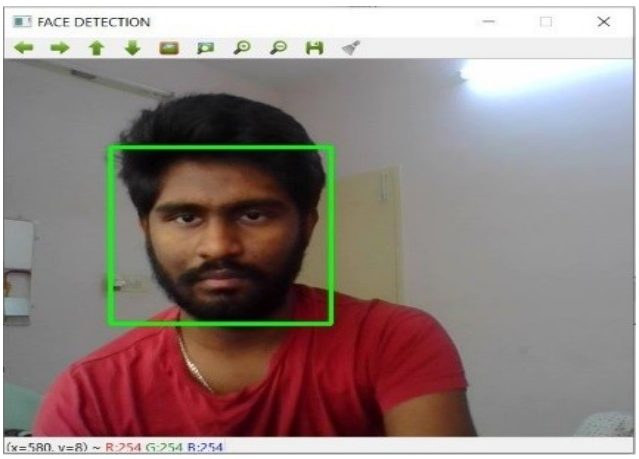
ATM'nin GPS konumu, Şekil 10'da gösterildiği gibi, ağır hasarlara neden olmasını önlemek için acil eylemler için.



Şekil 10. Polis merkezi ve itfaiye Polis merkezi ve itfaiye tarafından alınan kısa mesaj.



Şekil 11. ATM'ye erişen kullanıcılar için veritabanı.



Şekil 12. ATM'ye erişim sırasında kullanıcının yüzünün yakalanması.

ATM'ye giren kişileri takip etmek için, o kişinin yüzünü yakalamak için bir sinyal işleme tekniği kullanılır. ATM'ye yerleştirilen CCTV'nin görüntüsü daha fazla depolama alanı kaplar. Depolama alanını azaltmak için, ATM'yi kullanan çeşitli kişilerin yüzlerinin görüntülerini izlemek için python kullanıldı. ATM'ye yerleştirilen kamera, ATM'yi kullanan kişileri izler.

ATM'yi kullanıyor. Bunu uygulamak için python'daki "OpenCV" modülü kullanılmıştır. Haar özellik tabanlı Cascade sınıflandırıcı, bir görüntü veya videodaki nesneleri tanımlamak için nesne algılama algoritmasını kullanan kodda kullanılır. Program çalıştırıldığında, kamera sınıflandırıcıyı kullanarak yüz özellikleri yardımıyla bir yüz arar. Yüz tanındıktan sonra çevrilir, yeniden şekillendirilir ve vurgulanır. Yüzün etrafına dikdörtgen bir kutu çizilir ve veritabanına itilir. Kullanıcının yüzünün yakalanması Şekil 11'de ve tüm kullanıcıların görüntülerinin kaydedildiği konum Şekil 12'de gösterilmektedir. Böylece, bu özellikler bir ATM sisteminin etkili, güvenli ve kolay erişilebilir olmasının yolunu açmaktadır.

V. SONUÇ

Bu nedenle, önerilen bu sistem yetkilendirme için RFID kartını ve kullanıcının parmak izini kullanmıştır. Birden fazla hesap olması durumunda, her banka hesabı için farklı RFID kartları kullanılabilir. Kart okuyucunun yakınlığına en yakın kart mevcut işlem için dikkate alınacaktır. İşlemin geçerli olup olmadığına bakılmaksızın, kart sahibinin sicil numarası için kart sahiplerine GPS aracılığıyla konum, tarih ve saat hakkında mesajlar göndererek güvenliği artırır. Ayrıca, düzenli olarak ayarlanan bir kamera, ATM'deki karta kimin erişmeye çalıştığını kontrol eder ve bu da dolandırıcılık durumlarında yardımcı olur. Takılan sensörler ilgili departmanları anında uyardığı için kazaları ve soygunları önler. Prototip için elde edilen etkili sonuçlar, akıllı ATM için önerilen sistemi doğrulamaktadır.

Önerilen sistem, ATM'de uygulanmak üzere para transferi olanaklarının eklenebileceği bir ATM sisteminin sadece bir prototipidir. Kullanıcıya ATM'nin GPS konumunu, çekilen nakit miktarını göndermenin yanı sıra, kullanıcının yüzünün görüntüsü de gönderilebilir. ATM'de hırsızlık ve kazalara karşı güvenliği artırmak için yangın algılama ve hasar tespiti için daha hassas sensörler yerleştirilebilir [9], [10]. Parmak izi tanımada sahtekarlık Önerilen sistemde bu konuya yönelik güvenliği sağlamak için yüz tanıma, iris tarayıcı, OTP oluşturma gibi ekstra güvenlik önlemleri eklenebilir.

VI. REFERANSLAR

[1] Hota, Jyotiranjan. (2013). Hindistan'da ATM Endüstrisinin Büyümesi. CSI Communications. 36. 23-25.

[2] The Times of India, "Atm Suçları". Available: https://timesofindia.indiatimes.com/topic/Atm-Crimes [Accessed: May 08,2020].

[3] Christiawan, B. A. Sahar, A. F. Rahardian and E. Muchtar, "Fingershield ATM - ATM Security System using Fingerprint Authentication," International Symposium on Electronics and Smart Devices (ISESD), Bandung, 2018, pp. 1-6.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, s.68-73.

[4] S. Hazra, "Smart ATM Service," 2019 Devices for Integrated Circuit (DevIC), Kalyani, Hindistan, 2019, s. 226- 230.

[5] S. Sankhwar ve D. Pandey, "A Safeguard against ATM Fraud," 2016 IEEE 6th International Conference on Advanced Computing (IACC), Bhimavaram, 2016, s. 701-705, doi: 10.1109/IACC.2016.135.

[6] K. Archana, P. B. Reddy ve A. Govardhan, "Sensör ve kontrolörler yardımıyla ATM için güvenliği artırmak, " 2017 Uluslararası Enerji, İletişim, Veri Analitiği ve Yumuşak Hesaplama Konferansı (ICECDS), Chennai, 2017, s. 1012 -1015, doi: 10.1109/ICECDS.2017.8389590.

[7] V. M. E. Jacintha, S. J. Rani, J. G. Beula ve J. J. Johnsly, "ATM güvenlik sistemlerinin kapsamlı bir çözümü," 2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM), Chennai, 2017, pp.934-938, doi: 10.1109/ICONSTEM.2017.8261340.

[8] Rhydo Labz. R30X Serisi Parmak İzi Tanımlama Modülü Kullanım Kılavuzu. Mevcut: https://www.rhydolabz.com/documents/finger-print-module.pdf. [Erişim: 08 Mayıs 2020].

[9] P. A. Paresh ve Dr. Latha Parameswaran, "Akıllı binalarda yangın tespiti için görüş tabanlı algoritma", Lecture Notes in Computational Vision and Biomechanics içinde, cilt 30, Springer Hollanda, 2019, s. 1029-1038.

[10] V. Ashokan ve Murthy, O. V. R., "ATM'lerde anormal olay tespiti için sınıflandırıcıların karşılaştırmalı değerlendirmesi", 2017 Uluslararası Akıllı Hesaplama, Enstrümantasyon ve Kontrol Teknolojileri Konferansı, ICICICT 2017, 2018, cilt 2018-Ocak, s. 1330-1333.